CLAIMS

We claim:

1. A security system for computers, wherein said computers are at least one of a personal computer, a network server, a cellular phone, a palm pilot, a car computer, and/or other computerized gadget, comprising at least: A system for automatic segregation between programs that is applied to at least one of the hard disks and other non-volatile storage devices;

2. The system of claim 1 wherein said automatic segregation is used and at least one of the following exists:
    a. A monitoring and capturing system, which monitors at least one of storage devices and communications devices;
    b. A database of security rules, comprising at least one of: a set of default rules, a set of pre-distribution acquired rules that are good for many users of the selected operating system, and acquired additional user-defined rules; and
    c. A user interface, which can interact with the user in order to at least one of: learn acceptable behavior patterns, warn the user of perceived dangers, wait for his authorization whenever necessary, and allow the user to view and modify the database of authorizations.

3. The system of claim 2 wherein at least one of:
    a. Said user interface at least also warns the user explicitly in cases of potentially highly dangerous activities;
    b. Said database comprises also at least learned statistics of normal and reasonable behavior of programs in the user's computer;
    c. Said user interface at least also allows the user to view statistics of behavior of important programs and especially programs that are allowed to access communication channels, especially in what is related to sending and receiving data over the communication lines;

d. Said database comprises also at least a log of the questions that the Security System asked the user and his replies kept at least for a certain period; and
e. Said database comprises also at least, when needed, a log of suspicious activities detected kept at least for a certain period.

4. The system of claim 2 wherein the security rules and/or functions performed by the Security System comprise automatic segregation of programs into their natural environments and at least one of the following:
   a. Constantly monitoring the security-sensitive elements of the computer system, and mainly all relevant peripheral device activities, and especially storage devices and communication devices, and detecting and selectively intercepting security-sensitive behaviors, suspicious behaviors and dangerous behaviors and acting upon them in according with default and acquired sets of security rules;
   b. At least one of Warning the user and request for authorization and automatic interception for security-sensitive activities and especially any first-time attempts to access communication channels;
   c. Enabling the user to request at least one of automatic blocking and warning of the user of any attempts of external programs from the network to connect to the user's computer through the communication channels;
   d. Interception and more explicit warning of the user about potentially highly dangerous activities;
   e. Warning the user about significant statistical deviations from normal behaviors of applications and operating system and especially as relates to suddenly sending out large amounts of data;
   f. Enabling the user to request enforcing of at least one of additional limitations on the communication ports allowed to be opened and when needed also limitations on types of protocols allowed;
   g. Monitoring and intercepting as much as possible all attempts of applications to gain direct port accesses to security sensitive

devices and especially the storage media and the communication channels;

h. Implementing Virtual Shared data areas on the storage media, for at least one of temporary files and accessing keys in the registry and other files, so that programs are given the illusion that they are accessing the shared area, but in reality are each redirected to a separate private area; and

i. Pushing at least part of the operating system from the most privileged processor ring to a lower privilege ring and enabling needed functions to run in said lower privilege ring.

5. The system of claim 2 wherein said monitoring and capturing system includes also a hardware element which monitors hardware accesses, so that the Security System can discover events where access has been made to the security-sensitive ports, especially the storage media and the communication channels, without an apparent corresponding event on the system level as monitored by said Security System's software.

6. The system of claim 2 wherein said default automatic segregation is implemented so that, by default, each program is allowed to at least one of access, read, write, execute, create, and delete files only within its natural environment, and said natural environment is mainly the directory in which it is installed, its sub-directories, and - for reading only - non-strategic shared files, unless the program is explicitly given more rights.

7. The system of claim 1 wherein high security protected areas are at least one of: encrypted, marked with a finger print, and automatically backed up to as least one more area for additional safety.

8. The system of claim 2 wherein the communication devices include also at least one of USB devices, Bluetooth devices and other wireless devices, and/or wherein the monitoring of access to communication devices includes also protocols for sending Faxes.

9. A security method for computers, wherein said computers are at least one of a personal computer, a network server, a cellular phone, a palm pilot, a car computer, and/or other computerized gadget, comprising the

steps of using at least a method for automatic segregation between programs that is applied to at least one of the hard disks and other non-volatile storage devices.

10. The method of claim 9 wherein said automatic segregation is used and at least one of the following exists:
    a. Providing a monitoring and capturing system, which monitors at least one of storage devices and communications devices;
    b. Creating and maintaining a database of security rules, comprising at least one of: a set of default rules, a set of pre-distribution acquired rules that are good for many users of the selected operating system, and acquired additional user-defined rules; and
    c. Providing a user interface, which can interact with the user in order to at least one of: learn acceptable behavior patterns, warn the user of perceived dangers and wait for his authorization whenever necessary.

11. The method of claim 10 wherein at least one of:
    a. Said user interface at least also warns the user explicitly in cases of potentially highly dangerous activities;
    b. Said database comprises also at least learned statistics of normal and reasonable behavior of programs in the user's computer;
    c. Said user interface at least also allows the user to view statistics of behavior of important programs and especially programs that are allowed to access communication channels, especially in what is related to sending and receiving data over the communication lines;
    d. Said database comprises also at least a log of the questions that the Security System asked the user and his replies kept at least for a certain period; and
    e. Said database comprises also at least, when needed, a log of suspicious activities detected kept at least for a certain period.

12. The method of claim 10 wherein the security rules and/or functions performed by the Security System comprise automatic segregation of programs into their natural environments and at least one of the following:
    a. Constantly monitoring the security-sensitive elements of the computer system, and mainly all relevant peripheral device activities, and especially storage devices and communication devices, and detecting and selectively intercepting security-sensitive behaviors, suspicious behaviors and dangerous behaviors and acting upon them in according with default and acquired sets of security rules;
    b. At least one of Warning the user and request for authorization and automatic interception for security-sensitive activities and especially any first-time attempts to access communication channels;
    c. Enabling the user to request at least one of automatic blocking and warning of the user of any attempts of external programs from the network to connect to the user's computer through the communication channels;
    d. Interception and more explicit warning of the user about potentially highly dangerous activities;
    e. Warning the user about significant statistical deviations from normal behaviors of applications and operating system and especially as relates to suddenly sending out large amounts of data;
    f. Enabling the user to request enforcing of at least one of additional limitations on the communication ports allowed to be opened and when needed also limitations on types of protocols allowed;
    g. Monitoring and intercepting as much as possible all attempts of applications to gain direct port accesses to security sensitive devices and especially the storage media and the communication channels;
    h. Implementing Virtual Shared data areas on the storage media, for at least one of temporary files and accessing keys in the registry and other files, so that programs are given the illusion that they are accessing the shared area, but in reality are each redirected to a separate private area; and

i. Pushing at least part of the operating system from the most privileged processor ring to a lower privilege ring and enabling needed functions to run in said lower privilege ring.

13. A computer security system capable of automatic segregation of programs into their natural environments so that each program is allowed to at least one of access, read, write, execute, create, and delete files only within its natural environment, which is mainly the directory in which it is installed, its sub-directories, and - for reading only - non-strategic shared files, unless specifically given more rights.

14. A method of implementing security in computers by automatic segregation of programs into their natural environments so that each program is allowed to at least one of access, read, write, execute, create and delete files only within its natural environment, which is mainly the directory in which it is installed, its sub-directories, and - for reading only - non-strategic shared files, unless specifically given more rights.

15. The Security system of claim 1 wherein the computer is at least one of: cellular phone, car computer, and other computerized gadget, and wherein at least one of:

    a. Access to highly sensitive data, such as credit card details or private encryption keys, needs explicit permission by the user.
    b. Any attempt to automatically generate an outgoing communication needs explicit permission by the user.
    c. Any attempts to alter at least one of EMROMM and important system files and sensitive data, need explicit permission by the user.

16. The system of claim 1 wherein the user is an organization and at least some of the control over authorizations is in the hands of at least one of: at least one central authority, and the system administrator.

17. The system of claim 16 wherein the Security System of the central authority and/or of the system administrator performs also at least one of:

a. Automatically checking at least once in a while if the Security System is functioning properly on the other computers.
b. Noticing and intercepting communication attempts from computers where the amount of actual communication does not fit the amount reported by the Security System of that computer.

18. A security system wherein the communications device of each computer or group of computers is adapted to noticing and at least reporting back to at least one of the relevant computer, a central authority, and the system administrator about cases where the amount of actual communication does not fit the amount reported by the Security System of that computer.

19. The system of claim 1 wherein by default each program can only see itself and the operating system and the computer resources that it is allowed to see, so that it lives in a Virtual Environment (VE).

20. The system of claim 1 wherein the Security System also identifies if the user or the application initiated at least one of accessing a file outside the natural environment or virtual environment of the program, and other potential security-risk commands, and so can allow more flexibility and/or less limitations and/or no limitations if the command was initiated directly by the user than if it was initiated by the application.

21. The system of claim 20 wherein the Security System also makes sure that programs cannot create the false impression that certain actions were initiated by the user by falsifying user input through one of the input devices.

22. The system of claim 1 wherein the Security System also makes sure that when it requests authorization no other programs can enter false answers as if they were entered by the user through one of the input devices.

23. The system of claim 1 wherein in the cases where private keys are generated or stored by the browsers, additional rules are used in order to identify the directories where these keys are held.

24. The security system of claim 1 wherein the communications device of each computer is adapted to notice and at least report back to the computer about cases where the amount of actual communication does not fit the amount reported by the software of that computer.

25. The security system of claim 1 wherein the user is an organization and at least some of the control over authorizations is in the hands of at least one central authority, and the Security System on the central authority's computer and/or the communications device of each computer is adapted to notice and intercept communication attempts from computers where the amount of actual communication does not fit the amount reported by the at least one of: the software of that computer, and the operating system of that computer.

26. The security method of claim 9 comprising the steps of using a communications device of each computer which is adapted to notice and at least report back to the computer about cases where the amount of actual communication does not fit the amount reported by the software of that computer.

27. The security method of claim 9 wherein the user is an organization comprising the steps of using in each computer a communications device that is adapted notice and report back to the computer and/or to the central control about cases where the amount of actual communication does not fit the amount reported by the software of that computer.

28. The system of claim 1 wherein the Security System learns during the installation of new programs which files are related to them outside their directory tree.

29. The system of claim 1 wherein any attempts of programs, initiated by the programs, to exceed their natural environments are automatically blocked by the security system.

30. The system of claim 1 wherein the security system automatically blocks potentially highly dangerous activities or asks the user for explicit

authorization, even if the user supposedly allowed this to an application through the dialog box.

31. The security system of claim 1 wherein the communication with at least one of a keyboard and a mouse uses encryption in order to prevent falsifying user responses.

32. The security system of claim 31 wherein said encryption includes also a date & time stamp.

33. A security system in computers wherein the security system automatically blocks potentially highly dangerous activities or asks the user for explicit authorization, wherein said potentially highly dangerous activities are at least some of: formatting a drive, concurrent deletion of multiple files, changing hard disk partition information, changing boot area information, installing drivers in levels close to the kernel of the operating system, accessing the defined high-security areas, modifying or renaming executables that reside outside the natural environment of the offending executable programs, and changing the linking of file types with applications that will be run when clicking on them.

34. The system of claim 17 wherein the security system of each computer also encrypts the outgoing data packets with a unique identifier for each computer and reports also additional data identifying the packets that are being sent out, and so that at least one of the communication devices or the central authority can also find out if outgoing data packets have been changed.

35. The system of claim 18 wherein the security system also encrypts the outgoing data packets and reports also additional data identifying the packets that are being sent out, so that the communication devices can also find out if outgoing data packets have been changed.

36. The system of claim 24 wherein the security system also encrypts the outgoing data packets and reports also additional data identifying the packets that are being sent out, so that the communication devices can also find out if outgoing data packets have been changed

37. The system of claim 1 wherein if an application changes after being given certain permissions, the user is notified about and asked again for permissions or such changes are automatically prevented or the change application is automatically limited to a new VE.

38. The system of claim 1 wherein at least one of the following features exist:
    a. The security system intercepts the operating system the moment it is being loaded into memory and transfers it to a higher ring so that any attempt by the operating system to access ring 0 will cause a CPU exception, and in order to increase efficiency the security system rewrites on the fly each such command in the operating system code which is running in the computer's RAM to access instead the current ring in which it is in, so that the next time that line of code is accessed in memory, the exception will not occur anymore until the next boot.
    b. The security system transfers only physical device drivers to a less privileged ring in order to be able to control direct access to physical devices.
    c. The operating system itself transfers physical device drivers to a less privileged ring in order to be able to control direct access to physical devices.
    d. At least one of the physical device drivers and the operating system are still in ring 0 but there is at least one more privileged area within ring 0 which can catch exceptions caused by at least one of device drivers in ring 0 and the operating system itself.
    e. At least one of the physical device drivers and the operating system are still in ring 0 but there is at least one more privileged area below ring 0 which can catch exceptions caused by at least one of device drivers in ring 0 and the operating system itself

39. The system of claim 17 wherein the communication device is also capable of generating automatically various reports on outgoing and/or incoming data and the security system makes sure that no other applications can interfere with the device driver of the communication card and thus interfere with these reports.

40. The system of claim 18 wherein the communication device is also capable of generating automatically various reports on outgoing and/or incoming data and the security system makes sure that no other applications can interfere with the device driver of the communication card and thus interfere with these reports.

41. A security system for computers wherein at least one of the physical device drivers and the operating system are still in ring 0 but there is at least one more privileged area within ring 0 or below ring 0 which can catch exceptions caused by at least one of device drivers in ring 0 and the operating system itself

42. The system of claim 1 wherein at least one part of the security system becomes active even if the computer is booted from at least one of a floppy drive, CD, network drive, and any other source that is not the normal boot area.

43. The system of claim 42 wherein at least one of the following features exist:
    a. Said activation is done by at least one of the BIOS and the processor itself before the normal boot sequence begins.
    b. If the security system discovers that the BIOS has been compromised or corrupted, it can at least one of issue a warning and restore it from various preferably hidden backups.
    c. The security system can determine that the bios has been compromised or corrupted by at least one of: if it was changed without authorization according to a digital signature and if it starts to behave suspiciously.
    d. When changes need to be made in at least one of the security system itself and the BIOS, a physical key needs to be physically attached to at least one of the computer amd any of its peripheral devices.

44. The system of claim 1 wherein the Security System is an integral part of the operating system.

45. The system of claim 19 wherein if an application launches another application, the newly launched application is limited to the VE of the launching application.

46. The system of claim 1 wherein if users download many files into a single download directory, the security system at least one of: uses context sensitive information, and detects if a downloaded program starts looking at files that were downloaded at different times or starts going over the entire directory or tries to modify other executables in that directory.

47. The system of claim 1 wherein in order to protect the segregation of processes in memory, the Security System asks the user to explicitly authorize programs that he wants to allow to access APIs that allow accessing the memory of other processes.

48. The system of claim 1 wherein in order to prevent device drivers from accessing devices other then those that they are intended to access, each device driver must have a definite type indicator and is allowed to access only devices of the indicated type.

49. The system of claim 48 wherein each device driver is also prevented from accessing other device drivers that can access other types of devices.

50. The system of claim 1 wherein the security system replaces at least some of the Operating System's dialogue boxes and other components that can request input from the user, so that the Security System has more control on what is happening in them.

51. The system of claim 19 wherein programs are allowed to send OS messages only to programs which are running within their own Virtual Environments

52. The system of claim 1 wherein the Security system replaces at least some of the OS functions that deal with the OS message system, and attaches to each message an identification that shows if the OS or

another application is the source of the message, and the Security System allows certain messages to be initiated only by the OS.

53. A security system wherein the Security system replaces at least some of the OS functions that deal with the OS message system, and attaches to each message an identification that shows if the OS or another application is the source of the message, and the Security System allows certain messages to be initiated only by the OS.

54. The system of claim 20 wherein at least one of the following features exist:
    a. In order to prevent misleading textual questions the Security system uses also at least partial semantic analysis of what the user is really being asked, by at least one of: analyzing sentence structures or at least significant word combinations and/or using various rules and/or a statistical database of commonly used questions.
    b. In order to prevent misleading textual questions the Security system guards at least the top line title of the dialogue box, so the when it is an "open file" dialogue box, it will always say so clearly, and if it is a "save file" dialog box it will always say so clearly.
    c. A new protocol is introduced for dialogue boxes, in which only the security systems runs completely the dialogue box and the programs have to indicate in a more structured format, what they want exactly.
    d. The security system automatically blocks potentially highly dangerous activities or asks the user for explicit authorization, even if the user supposedly allowed this to an application through the dialog box.

55. The system of claim 1 wherein the security system knows automatically about at least some highly important user files and directories.

56. The system of claim 55 wherein at least one of the following features exist:

a. Said files are at least one of ".doc" files and source code files, and said directories are at least directories containing such files, at least if these files were created by the user.
b. The security system can identify strategic files and/or directories by at least one of: using predefined rules; automatically marking programs as highly strategic according to the number and/or types of authorizations they have and/or by the fact that the user is using them interactively more than other programs or files or directories; and allowing the user explicitly to mark certain directories and/or certain file name extensions as highly protected.
c. The user is explicitly warned by the security system about attempts of programs to access highly important user files or directories even if the user supposedly allowed the program to access them through the dialogue box – if the program is not normally associated with such files or directories.

57. The system of claim 19 wherein installed drivers can also be associated with Virtual Environments, and thus limited in the scope of their actions.

58. The system of claim 1 wherein the security system prevents running processes from at least one of: Changing their code in memory, and Changing the disk file of their executable code.

59. The system of claim 1 wherein at least one of programs that can access the Internet, Browsers, important Operating system files, and other highly strategic programs, cannot be changed or cannot run EVEN if the user authorizes the change directly to the Security System, unless the update or patch carries a digital certificated that proves that it is indeed an authorized and unchanged official patch by the vendor who made the original program.

60. The system of claim 1 wherein the security system also prevents applications from accessing directly lower level functions that can access devices except by calling them through the normal kernel interface.

61. The system of claim 19 wherein at least one of the following features exist:
    a. Unless explicitly given additional rights by the user all of the actions initiated by a program are automatically limited to the scope of its own VE.
    b. When a new program is being installed the user has the option of choosing a new VE for that program, or allowing it to become an update of an already existing VE, or allowing it to have free access to the entire computer.
    c. The user is able to correct mistakes, at least for a certain time, by undoing the installation of programs, at least when they are installed in a limited VE.
    d. If shared drives are allowed, only the user is allowed to access files on shared drives on other computers, or each program is allowed to see and access in each shared drive only the same VE that it has on its own computer.
    e. If the user allows a newly installing program to inherit or overwrite an existing VE, the security system first creates a virtual private environment copy of the modified directories, at least for a certain period, so that the user can still request to undo this if he made a mistake, at least for a certain period.
    f. The security system backs up all the changed files or directories at least for a certain time and/or keeps a rollback log of all changes that were made to the relevant files and directories or even of all changes anywhere in at least one of the hard disk and other non-volatile storage devices, in order to enable the undo if the user needs it.
    g. Even when the user allows a program to be installed without VE limitations, any changes in the entire hard disk after or during the installation, are completely undo-able at least for a certain time period.
    h. Even if the user requested installation without VE limitation, the new program is first installed in a separate VE, and only after a certain time period or after the user authorizes it (and/or for example after the security system checks various parameters to see that things seem ok), the VE limitations are lifted or this VE is merged with the unlimited VE.

62. The system of claim 1 wherein any changes that happen on at least one of the hard disk and other nonvolatile storage devices and other connected media are completely undo-able at least for a certain time period, by keeping a rollback log of all changes or of all significant changes.

63. The system of claim 1 wherein the security system can identify at least one of strategic files and strategic directories by at least one of: using predefined rules; automatically marking programs as highly strategic according to the number and/or types of authorizations they have and/or by the fact that the user is using them interactively more than other programs or files or directories; and allowing the user explicitly to mark certain directories and/or certain file name extensions as highly protected.

64. The system of claim 1 wherein at least one of the Security System and the Operating system can alert the user and/or automatically prevent or take action if a malicious program tries to misuse at least one of the CPU resources, the free RAM memory, and the free space of the disk and/or other non-volatile storage devices and/or if it creates on purpose an artificial load on disk activity, and wherein at least one of the following is done:
    a. Taking over the free disk space is prevented by a default quota for each newly installed application, which can be changed by the user if needed.
    b. Creating false load on the disk activity can be prevented by detecting automatically suspect behaviors.
    c. The Security System and/or the Operating System automatically shows to the user and/or to the administrator in an organization, whenever any of the CPU and/or RAM resources become too low, or whenever significant deviations from normal statistics in this resources are detected, at least one of: Which applications are taking up most of these resources, the percent they are using, and, to the extent possible, what they are doing, and the VE of these processes.
    d. Automatically detecting by at least one of software and hardware in the CPU itself at least one of entering the CPU into useless loops and other suspect activities in the CPU.

e. The OS or the Security System requests authorization from the user if a program requests Real-time priority or any other priority that can significantly slow down other processes, at least the first time it tries to get such priority or unless the user gives it such a privilege from then on.

65. The system of claim 1 wherein at least one of the following features exists:
    a. The CPU has hardware support for automatically refusing to execute any code which is in an area defined as data.
    b. The CPU refuses to return from the stack to addresses that are outside the memory area of the program's code

66. The system of claim 1 wherein the hardware of the CPU and/or the hardware of the disk itself does not allow any access to a file unless the software that tries to access it is identified as its rightful owner, by at least one of providing the appropriate password, and other means.